FICAM Testing Program Functional Requirements and Test Cases

VERSION 0.1.3

DRAFT

FIPS 201 EVALUATION PROGRAM

May 6, 2013

Office of Government wide Policy
Office of Technology Strategy
Identity Management Division
Washington, DC 20405

Document History

Status	Version	Date	Comment	Audience
Draft	0.0.1	4/24/2013	Document creation	Limited
Draft	0.0.2	4/30/2013	Added background and objectives text, normative references	Limited
Draft	0.1.0	4/30/2013	Full comment resolution version for review	Limited
Draft	0.1.1	5/1/2013	Release candidate 1	Limited
Draft	0.1.2	5/2/2013	Revised per May 1, 2013 EPTWG Meeting	Limited
Draft	0.1.3	5/6/13	Draft Release	EPTWG

Table of Contents

1 Background

The General Services Administration (GSA) is responsible for supporting the adoption of interoperable and standards-based Identity, Credential, and Access Management (ICAM) technologies throughout the Federal Government. As part of that responsibility, GSA operates and maintains the Federal Information Processing Standard (FIPS) 201 Evaluation Program (EP) and its FIPS 201 Approved Products List (APL), as well as services for Federal ICAM (FICAM) conformance and compliance. GSA is currently transitioning the FIPS 201 EP and APL into the enhanced GSA FICAM Testing Program.

2 Objectives

This document identifies the functional requirements that the GSA FICAM Testing Program will perform on Physical Access Control Systems (PACS) submitted for evaluation. All requirements are instrumented using a smart card as presented to the system and various PKI paths. The PKI and smart cards test for specific common failures in cards and PKI, as well as Advanced Persistent Threat (APT) issues that impact PACS specifically. The PACS evaluation process is designed to be agnostic to architecture, and focuses solely on functional testing using an end-to-end testing methodology.

3 Test Instrumentation

The FICAM Testing Program for PACS relies on fully-defined, instrumented testing. This requires two core elements:

1. *ICAM Test Cards* – There are two cards that are completely valid and well formed. In addition, there are cards that have injected faults assuming both day-to-day operational errors as well as cards from a well-funded attacker.
2. *Test PKI* – This PKI provides the ability to link golden test cards with PKI faults. This provides the mechanism needed to verify that the system under test honors the PKI.

The full testing program, leveraging these test instruments, is described in *Appendix 1*.

3.1 ICAM Cards Used in Test

The following cards are used in the FICAM Testing Program.

1. Live PIV and PIV-I Cards from various issuers;
2. ICAM Test Cards (detailed in Table 1);
3. NIST PIV Test Cards; and
4. DoD JITC CAC Test Cards.

Table 1 - ICAM Test Cards Used in Test

ICAM Test Cards	Description	Threat Type
1	Golden PIV	None
2	Golden PIV-I	None
3	**Placeholder for ECC card**	TBD
4	Tampered CHUID	Manipulated Data
5	Tampered PIV and Card Authentication Certificates	Manipulated Data
6	Tampered PHOTO	Manipulated Data
7	Tampered FINGERPRINT	Manipulated Data
8	Tampered SECURITY OBJECT	Manipulated Data
9	Expired CHUID signer	Invalid Date
10	Expired certificate signer	Invalid Date
11	PIV Authentication Certificate expiring after CHUID	Invalid Date
12	Authentication certificates valid in future	Invalid Date
13	Expired authentication certificates	Invalid Date
14	Expired CHUID	Invalid Date
15	Valid CHUID copied from one card to another **(PIV)**	Copied Credential
16	Valid Card Authentication Certificate copied from one card to another **(PIV)**	Copied Credential
17	Valid PHOTO copied from one card to another **(PIV)**	Copied Credential
18	Valid FINGERPRINT copied from one card to another **(PIV)**	Copied Credential
19	Valid CHUID copied from one card to another **(PIV-I)**	Copied Credential
20	Valid Card Authentication Certificate copied from one card to another **(PIV-I)**	Copied Credential
21	Valid PHOTO copied from one card to another **(PIV-I)**	Copied Credential
22	Valid FINGERPRINT copied from one card to another **(PIV-I)**	Copied Credential
23	Private and Public Key mismatch	No Trusted Path
24	Revoked authentication certificates	Revoked Credential

3.2 PKI Used in Test

Table 2 details the PKI infrastructure used for the FICAM Testing Program.

Table 2 - PKI Used in Test

Path Number	Fault description	Operational group
1	Invalid CA Signature	Manipulated Data
2	Invalid CA notBefore Date	Revoked/Date Invalid
3	Invalid CA notAfter Date	Revoked/Date Invalid
4	Invalid Name Chaining	Standards Conformant Processing
5	Missing Basic Constraints	Standards Conformant Processing
6	Invalid CA False Critical	Manipulated Data
7	Invalid CA False not Critical	Standards Conformant Processing
8	Invalid pathLenConstraint	Standards Conformant Processing
9	keyUsage keyCertSign not set	Standards Conformant Processing
10	keyUsage Not Critical	Standards Conformant Processing
11	keyUsage Critical cRLSign False	Standards Conformant Processing
12	Invalid inhibitPolicyMapping	Standards Conformant Processing
13	Invalid DN nameConstraints	Standards Conformant Processing
14	Invalid Subject Alternative Name	Standards Conformant Processing
15	Invalid Missing CRL	Standards Conformant Processing
16	Invalid Revoked CA	Revoked/Date Invalid
17	Invalid CRL Signature	Manipulated Data
18	Invalid CRL Issuer Name	Standards Conformant Processing
19	Invalid Old CRL nextUpdate	Revoked/Date Invalid
20	Invalid CRL notBefore Date	Revoked/Date Invalid
21	Invalid distributionPoint	Standards Conformant Processing
22	Valid requiredExplicitPolicy	Standards Conformant Processing
23	Invalid requiredExplicitPolicy	Standards Conformant Processing
24	Valid GeneralizedTime	PKI/Crypto Compatibility
25	Invalid GeneralizedTime	Standards Conformant Processing

Path Number	Fault description	Operational group
26	ECC prime256v1	PKI/Crypto Compatibility
27	ECC secp384r1	PKI/Crypto Compatibility
28	Invalid ECC Signature p256	Manipulated Data
29	Invalid Policy Mapping p256	Standards Conformant Processing
30	Invalid ECC Signature	Manipulated Data
31	Invalid Policy Mapping	Standards Conformant Processing
32	Invalid SKID	Standards Conformant Processing
33	Invalid AKID	Standards Conformant Processing
34	Invalid CRL format	Standards Conformant Processing
35	4096 RSA key	PKI/Crypto Compatibility

4 Normative References

[Common] FPKIPA X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework, Version 3647 - 1.17, December 9, 2011

[E-PACS] FICAM Personal Identity Verification (PIV) in Enterprise Physical Access Control Systems (E-PACS), DRAFT Version 2.0.2, May 24, 2012

[FBCA] FBCA X.509 Certificate Policy For Federal Bridge Certification Authority (FBCA), Version 2.25, December 9, 2011

[FIPS 201] FIPS 201-1

[HSPD-12] Homeland Security Presidential Directive 12, August 27, 2004

[M-06-18] OMB Memorandum 06-18, June 30, 2006

[M-11-11] OMB M-11-11, February 3, 2011

[Roadmap] FICAM Roadmap and Implementation Guidance, Version 2.0, December 2, 2011

[SP800-73] NIST SP 800-73-3, Parts 1-3, February 2010

[SP800-76] NIST SP 800-76-1, January 2007

[SP800-78] NIST SP 800-78-3, December 2010

[SP800-96] NIST SP 800-96, September 2006 {revision post FIPS 201-2}

[UL 294] The Standard of Safety for Access Control System Units, UL Edition Number – 5, Date 01/29/1999, Type ULSTD

[UL 1076] The Standard of Safety for Proprietary Alarm Units, UL Edition Number – 5, Date 09/29/1995, Type ULSTD

[UL 1981] The Standard for Central-Station Automation Systems UL Edition Number -2, Date 06/30/2003, Type ULSTD

Appendix 1 Functional Requirements and Test Cases

1	Scoring Guidelines
	Security - A control directly impacting security of the system.
	Usability - A control impacting end user system usability. Does not directly impact security.
	Required - Must be present. Must work correctly: Red/Green.
	Optional - May be present. If present, it must work correctly: Red/Green. Not present: Yellow.

			2	**Requirements at Time of In-Person Registration In Accordance With [E-PACS] PIA-9**	*All tests use PKI-AUTH unless specifically noted.* *All tests using a CONTACT reader unless specifically noted.*	*Note all requirements sourced from [E-PACS] unless otherwise noted.*
Security/ Usability	**Required/ Optional**	**Test #**	**Test**	**Requirement**	**Test Case: Pass/Fail criteria**	**Requirement Source**
			2.1	**Signature Verification**		
Security	Required	1	2.1.1	Verify products ability to validate signatures in the certificates found in the certification path for a PIV credential	Card 1: PIV Golden Registers successfully.	PIA-2 thru PIA-7
Security	Required	2	2.1.2	Verify products ability to validate signatures in the certificates found in the certification path for a PIV-I credential	Card 2: PIV-I Golden Registers successfully	PIA-2 thru PIA-7
Security	Required	3	2.1.3	Verify products ability to recognize invalid signature on an intermediate CA in the certification path	Card 1: (Golden PIV Card) w/ PKI Fault Bridge 2.1.2 fails to register successfully.	PAI-3.2, PIA-3.4, PIA-4, PIA-5
Security	Required	4	2.1.4	Verify products ability to recognize invalid signature on the End Entity certificate	Card 5: invalid PIV/Card Auth Signer fails to register successfully.	PAI-3.2, PIA-3.4, PIA-4
Security	Required	5	2.1.5	Verify products ability to recognize certificate/private key mismatch	Card 23: Certificate Private Key mismatch fails to register successfully.	PAI-3.2, PIA-3.4, PIA-4
			2.2	**Certificate Validity Periods**		

Security	Required	6	2.2.1	Verify products ability to reject a credential when notBefore date of the intermediate CA certificate is sometime in the future	Card 1: (Golden PIV Card) w/ PKI Fault Bridge 2.2.1 fails to register successfully.	PIA-3.5, PIA-5
Security	Required	7	2.2.2	Verify products ability to reject a credential when notAfterDate of the End Entity Signing CA is sometime in the past.	Card 10: expired signing CA fails to register successfully.	PAI-3.2, PIA-3.4, PIA-4
Security	Required	8	2.2.3	Verify products ability to reject a credential when notBefore date of the End Entity certificate is sometime in the future	Card 12: (Certs not yet valid) fails to register successfully.	PIA-3.5
Security	Required	9	2.2.4	Verify products ability to reject a credential when notAfter date of the intermediate certificate is sometime in the past	Card 1: (Golden PIV Card) w/ PKI Fault Bridge 2.2.3 fails to register successfully.	PIA-3.5, PIA-5
Security	Required	10	2.2.5	Verify products ability to reject a credential when notAfter date of the End Entity certificate is sometime in the past	Card 13: (Certs Expired) fails to register successfully.	PIA-3.5
			2.3	**Name Chaining**		
Security	Required	11	2.3.1	Verify products' ability to reject a credential when common name portion of the of the issuer's name in the End Entity certificate does not match common name portion of subject's name in the previous intermediate certificate	Card 1: (Golden PIV Card) w/ PKI Fault Bridge 2.3.1 fails to register successfully.	PIA-3.2, PIA-5
			2.4	**Basic Constraints Verification**		
Security	Required	12	2.4.1	Verify product's ability to recognize when the intermediate CA certificate is missing basicConstraints extension.	Card 1: (Golden PIV Card) w/ PKI Fault Bridge 2.4.1 fails to register successfully.	PIA-3.2, PIA-5

Security	Required	13	2.4.2	Verify product's ability to recognize when the basicConstraints extension is present and critical in the intermediate CA certificate but the CA component is false	Card 1: (Golden PIV Card) w/ PKI Fault Bridge 2.4.2 fails to register successfully.	PIA-3.2, PIA-5
Security	Required	14	2.4.3	Verify product's ability to recognize when the basicConstraints extension is present and not critical in the intermediate CA certificate but the CA component is false	Card 1: (Golden PIV Card) w/ PKI Fault Bridge 2.4.3 fails to register successfully.	PIA-3.2, PIA-5
Security	Required	15	2.4.4	Verify product's ability to recognize when the first certificate in the path includes basicConstraints extension with a pathLenConstraint of 0 (this prevents additional intermediate certificates from appearing in the path). The first certificate is followed by the second intermediate CA certificate and an End Entity certificate.	Card 1: (Golden PIV Card) w/ PKI Fault Bridge 2.4.4 fails to register successfully.	PIA-3.2, PIA-5
			2.5	**Key Usage Verification**		
Security	Required	16	2.5.1	Verify products ability to recognize when the intermediate certificate includes a critical keyUsage extension in which keyCertSign is false	Card 1: (Golden PIV Card) w/ PKI Fault Bridge 2.5.1 fails to register successfully.	PIA-3.2, PIA-5
Security	Required	17	2.5.2	Verify products ability to recognize when the intermediate certificate includes a non-critical keyUsage extension	Card 1: (Golden PIV Card) w/ PKI Fault Bridge 2.5.2 fails to register successfully.	PIA-3.2, PIA-5
Security	Required	18	2.5.3	Verify products ability to recognize when the intermediate certificate includes a critical keyUsage extension in which cRLSign is false	Card 1: (Golden PIV Card) w/ PKI Fault Bridge 2.5.3 fails to register successfully.	PIA-3.2, PIA-5
			2.6	**Certificate Policies**		

Security	Required	19	2.6.1	With the trust anchor set to Common Policy check to see if the validation software is able to recognize when an explicit certificate policy is required and present in the certificate path. The explicit policy will be set to PIV Hardware.	Production PIV registers successfully	PIA-3.2, PIA-5
Security	Required	20	2.6.2	With the trust anchor set to Common Policy check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the certificate path. The explicit policy will be set to an arbitrary value that is not present in the certificate path (ex., OID value 1.2.3.4).	Production PIV fails to register	PIA-3.2, PIA-5
Security	Required	21	2.6.3	With the trust anchor set so the certificate path requires trust across the Federal Bridge to the CertiPath Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and present in the certificate in a bridged trust environment. The explicit policy will be set to Medium Hardware. Test Condition: production PIV passes	Production PIV registers successfully	PIA-3.2, PIA-5
Security	Required	22	2.6.4	With the trust anchor set so the certificate path requires trust across the Federal Bridge to the CertiPath Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the certificate in a bridged trust environment. The explicit policy will be set to an arbitrary value that is not present in the certificate chain (ex., OID value 1.2.3.4).	Production PIV fails to register	PIA-3.2, PIA-5

Security	Required	23	2.6.5	With Common Policy anchor, check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the certificate - however, is present somewhere in the certificate path. The explicit policy will be set to a value that is present in the certificate path, but does not map to the end entity certificate (ex, High Hardware).	Production PIV fails to register	PIA-3.2, PIA-5
			2.7	**Inhibit Policy Mappings**		
Security	Required	24	2.7.1	The first intermediate certificate asserts NIST-test-policy-1 and includes a policyConstraints extension with inhibitPolicyMapping set to 0. The second intermediate certificate asserts Policy A and maps Policy A to Policy B. The end entity certificate asserts Policy A and Policy B	Card 1: (Golden PIV Card) w/ PKI Fault Bridge 2.9.1 fails to register successfully.	PIA-3.2, PIA-5
			2.8	**Name Constraints**		
Security	Required	25	2.8.1	The system recognizes when the intermediate certificate includes a nameConstraints extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls within that subtree.	Card 1: (PIV Golden) access grant succeeds	PIA-3.2, PIA-5
Security	Required	26	2.8.2	The system recognizes when the intermediate certificate includes a nameConstraints extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls outside that subtree.	Card 1: (Golden PIV Card) w/ PKI Fault Bridge 2.10.2 fails to register successfully.	PIA-3.2, PIA-5

Security	Required	27	2.8.3	The system recognizes when the intermediate certificate includes a nameConstraints extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls within that subtree and subjectAltName with a DN that falls outside that subtree.	Card 1: (Golden PIV Card) w/ PKI Fault Bridge 2.10.1 fails to register successfully.	PIA-3.2, PIA-5
			2.9	**Certificate Revocation Tests (CRL)**		
Security	Required	28	2.9.1	The system recognizes when no revocation information is available for the End Entity certificate	Card 1: (Golden PIV Card) fails access grant w/ PKI Fault Bridge 2.11.1	PIA-3.5, PIA-5, PIA-7
Security	Required	29	2.9.2	The system recognizes when a second intermediate CA certificate is revoked	Card 1: (Golden PIV Card) w/ PKI Fault Bridge 2.11.2 fails to register successfully.	PIA-3.5, PIA-5, PIA-7
Security	Required	30	2.9.3	The system recognizes when the End Entity certificate is revoked	Card 24: (Revoked status) fails to register successfully.	PIA-3.5, PIA-5, PIA-7
Security	Required	31	2.9.4	The system recognizes when a certificate in the path links to a CRL issued by a CA other than that which issued the cert	Card 1: (Golden PIV Card) w/ PKI Fault Bridge 2.11.5 fails to register successfully.	PIA-3.5, PIA-5, PIA-7
Security	Required	32	2.9.5	The system recognizes when a certificate in the path points to a CRL with an expired nextUpdate value	Card 1: (Golden PIV Card) w/ PKI Fault Bridge 2.11.6 fails to register successfully.	PIA-3.5, PIA-5, PIA-7
Security	Required	33	2.9.6	The system recognizes when a certificate in the path points to a CRL with a notBefore Date in the future.	Card 1: (Golden PIV Card) w/ PKI Fault Bridge 2.11.7 fails to register successfully.	PIA-3.5, PIA-5, PIA-7
Security	Required	34	2.9.7	The system recognizes when a certificate in the path has an incorrect distribution point	Card 1: (Golden PIV Card) w/ PKI Fault Bridge 2.11.8 fails to register successfully.	PIA-3.5, PIA-5, PIA-7
			2.10	**CHUID Verification**		

Security	Required	35	2.10.1	The system recognizes when the CHUID signature is invalid and does not verify	Card 4: (Invalid CHUID Signature) fails to register successfully.	PIA-3.2, PIA-4
Security	Required	36	2.10.2	The system recognizes when the CHUID signer certificate is expired	Card 9: (Expired CHUID signer) fails to register successfully.	PIA-3.6, PIA-5
Security	Required	37	2.10.3	The system recognizes when the CHUID is expired	Card 14: (Card Expired) fails to register successfully	PIA-3.6
Security	Required	38	2.10.4	The system recognizes when the FASC-N in the CHUID does not equal the FASC-N in the PIV Auth Cert	Card 15: (FASC-N in CHUID !=) fails to register successfully	PIA-3.2; [SP800-73], Part 1, §3.1.2
Security	Required	39	2.10.5	The system recognizes when the UUID in the CHUID does not equal the UUID in the PIV-I Auth Cert	Card 19: (UUID in CHUID !=) fails to register successfully	PIA-3.2; [SP800-73], Part 1, §3.3
Security	Required	40	2.10.6	The system recognizes when the PKI-AUTH certificate expires after the CHUID expiration date.	Card 11: (PKI-AUTH Cert after CHUID) fails to register successfully	[FIPS 201]; [FBCA] §6.3.2, Appendix A (10) & (11)
			2.11	**Facial Image Verification**	Need CHUID content signer? Or SecObj? Or in facial buffer?	
Security	Required	41	2.11.1	The system recognizes when the Facial Image signature is invalid and does not verify.	Card 6: (bad photo signature) fails to register successfully	PIA-3.2, PIA-4
			2.12	**Copied Containers**		
Security	Required	42	2.12.1	The system recognizes when the FASC-N in the PKI-CAK certificate does not equal the FASC-N in the PIV Auth Cert	Card 16: (FASC-N in PKI-CAK Cert !=) fails to register successfully	PIA-3.2; [SP800-73], Part 1, §3.1.2
Security	Required	43	2.12.2	The system recognizes when the UUID in the PKI-CAK certificate does not equal the UUID in the PIV-I Auth Cert	Card 20: (UUID in PKI-CAK Cert !=) fails to register successfully	PIA-3.2; [SP800-73], Part 1, §3.1.2

Security	Required	44	2.12.3	The system recognizes when the FASC-N in the Facial Image does not equal the FASC-N in the PIV Auth Cert	Card 17: (FASC-N in Facial Image !=) fails to register successfully	PIA-3.2; [SP800-73], Part 1, §3.1.2
Security	Required	45	2.12.4	The system recognizes when the UUID in the Facial Image does not equal the UUID in the PIV-I Auth Cert	Card 21: (UUID in Facial Image !=) fails to register successfully	PIA-3.2; [SP800-73], Part 1, §3.1.2
			2.13	**FINGERPRINT Verification**	If BIO Auth Meth is Supported at time of registration, tests in this section are Required. If content signer certificate is from CHUID, Section 2.10 is Required.	
Security	Required	46	2.13.1	The system recognizes when the Fingerprint signature is invalid and does not verify (using CHUID content signer certificate).	Card 7: (bad fingerprint signature) fails to register successfully	PIA-3.2, PIA-4
Security	Required	47	2.13.2	The system recognizes when the Fingerprint signature is invalid and does not verify (using biometric object signer certificate).	Card tbd: (bad fingerprint signature) fails to register successfully	PIA-3.2, PIA-3.4, PIA-3.5, PIA-3.6, PIA-4, PIA-5
Security	Required	48	2.13.3	Verify Product's ability to accept a valid credential with a matching fingerprint.	A good credential is presented to the system with a valid fingerprint object on card. System is presented correct bearer's fingerprint. Registration succeeds.	PIA-3 thru PIA-7
Security	Required	49	2.13.4	Verify Product's ability to reject a valid credential with a non-matching fingerprint.	A good credential is presented to the system with a valid fingerprint object on card. System is presented incorrect bearer's fingerprint. Registration fails.	PIA-3.3
Security	Required	50	2.13.5	The system recognizes when the FASC-N in the Fingerprint does not equal the FASC-N in the PIV Auth Cert	Card 18: (FASC-N in Fingerprint !=) fails to register successfully	PIA-3.2; [SP800-73], Part 1, §3.1.2

Security	Required	51	2.13.6	The system recognizes when the UUID in the Fingerprint does not equal the UUID in the PIV-I Auth Cert	Card 22: (UUID in Fingerprint !=) fails to register successfully	PIA-3.2; [SP800-73], Part 1, §3.1.2
			2.14	**Security Object Verification**	If Security Object is Supported, tests in this section are Required.	
Security	Required	52	2.14.1	The system recognizes when the Security Object signature is invalid and does not verify.	Card 8: (bad security object signature) fails to register successfully	PIA-3.4, PIA-4, PIA-5
			2.15	OCSP Response Checking		
Security	Required	53	2.15.1	The system successfully validates a good credential using an OCSP response with a good signature	Card 1: Golden PIV registers successfully	PIA-3.2, PIA-3.5
Security	Required	54	2.15.2	Validation fails using an OCSP responder with an expired signature certificate for a good card.	Card 1: Golden PIV fails to register successfully	PIA-3.2 PIA-3.5, PIA-3.6
Security	Required	55	2.15.3	Validation succeeds using an OCSP responder with a revoked signature certificate for a good card with PKIX_OCSP_NOCHECK present.	Card 1: Golden PIV registers successfully	PIA-3.2, PIA-3.5
Security	Required	56	2.15.4	Validation fails using an OCSP responder with a revoked signature certificate for a good card without PKIX_OCSP_NOCHECK present.	Card 1: Golden PIV fails to register successfully	PIA-3.2, PIA-3.5, PIA-3.6
Security	Required	57	2.15.5	Validation fails using an OCSP responder with a signature certificate containing an invalid signature for a good card.	Card 1: Golden PIV fails to register successfully	PIA-3.2, PIA-4
			2.16	**Interoperability Testing**	Tests in this section attempt to use a variety of dual interface and dual-chip production PIV and PIV-I cards in the system.	Note, should we add dual-chip here? See new dual-chip/NFC section.

Usability	Required	58	2.16.1	Various valid PIV (including CAC) and PIV-I cards can be individually registered using PKI-AUTH method.	PIV (including CAC) and PIV-I cards register successfully	PIA-6
			2.17	**Cryptography testing**	As stated, there is no context for challenge/response vs. use of crypto w/in certs and path for sigval. The FICAM Testing Program will isolate these two variables in new test cases.	
Security	Required	59	2.17.1	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (1024).	NIST card#7 registers successfully.	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5
Security	Required	60	2.17.2	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (2048).	NIST card#1 registers successfully.	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5
Security	Required	61	2.17.3	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (3072).	TBD	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5
Security	Optional	62	2.17.4	Verify Product's ability to validate signatures using RSASSA-PSS (1024).	TBD (valid through 1/1/2014)	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5

Security	Optional	63	2.17.5	Verify Product's ability to validate signatures using RSASSA-PSS (2048).	NIST card#2 registers successfully.	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5
Security	Optional	64	2.17.6	Verify Product's ability to validate signatures using RSASSA-PSS (3072).	TBD	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5
Security	Optional	65	2.17.7	RSA Key Transport (1024)	TBD (valid through 1/1/2014)	[SP800-78] Table 3-1
Security	Optional	66	2.17.8	RSA Key Transport (2048)	TBD	Derived from [SP800-78] Table 3-1 and [Common] §6.1.5
Security	Optional	67	2.17.9	RSA Key Transport (3072)	TBD	Derived from [SP800-78] Table 3-1 and [Common] §6.1.5
Security	Required	68	2.17.10	Verify Product’s ability to validate signatures using ECDSA (P-256)	NIST card#4 registers successfully.	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5

Security	Optional	69	2.17.11	Verify Product's ability to validate signatures using ECDSA (P-384)	NIST card#5 registers successfully.	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5
Security	Optional	70	2.17.12	ECDH (P-256)	TBD	[SP800-78] Table 3-1; [Common] §6.1.5
Security	Optional	71	2.17.13	ECDH (P-384)	TBD	[SP800-78] Table 3-1; [Common] §6.1.5
Security	Optional	72	2.17.14	Verify Product's ability to validate signatures using SHA-1	NIST card#7 registers successfully.	[SP800-78] Table 3-7; [Common] §6.1.5
Security	Required	73	2.17.15	Verify Product's ability to validate signatures using SHA-256	NIST card#1 registers successfully.	[SP800-78] Table 3-7; [Common] §6.1.5
Security	Optional	74	2.17.16	Verify Product's ability to validate signatures using SHA-384	NIST card#5 registers successfully.	[SP800-78] Table 3-7; [Common] §6.1.5
Security	Optional	75	2.17.17	Verify Product's ability for SYM-CAK using AES-128	TBD	[SP800-73] table 3-1; [Common] §6.1.5

Security	Optional	76	2.17.18	Verify Product's ability for SYM-CAK using AES-192	TBD	[SP800-73] table 3-1; [Common] §6.1.5
Security	Optional	77	2.17.19	Verify Product's ability for SYM-CAK using AES-256	TBD	[SP800-73] table 3-1; [Common] §6.1.5
Security	Optional	78	2.17.20	Verify Product's ability for SYM-CAK using 2TDEA	TBD	[SP800-73] table 3-1; [Common] §6.1.5
Security	Optional	79	2.17.21	Verify Product's ability for SYM-CAK using 3TDEA	TBD	[SP800-73] table 3-1; [Common] §6.1.5
Security	Required	80	2.17.22	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (2048) w/exponent of 65,537.	NIST card#1 registers successfully.	[SP800-78] Table 3-2
Security	Optional	81	2.17.23	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (2048) w/exponent of 2^256-1.	TBD	[SP800-78] Table 3-2
				Dual Chip Card	All new requirements/tests	[FIPS 201] allows dual chip cards.
			2.17	**CHUID Verification (Contactless chip on a 2 chip card)**	**These tests are run using a contactless reader**	

Security	Required	82	2.17.1	The system recognizes when the CHUID signature is invalid and does not verify	Card 4: (Invalid CHUID Signature) fails to register successfully.	PIA-3.2, PIA-4
Security	Required	83	2.17.2	The system recognizes when the CHUID signer certificate is expired	Card 9: (Expired CHUID signer) fails to register successfully.	PIA-3.6, PIA-5
Security	Required	84	2.17.3	The system recognizes when the CHUID is expired	Card 14: (Card Expired) fails to register successfully	PIA-3.6
Security	Required	85	2.17.4	The system recognizes when the PKI-CAK certificate expires after the CHUID expiration date.	Card 11: (PKI-CAK Cert after CHUID) fails to register successfully	[FIPS 201]; [FBCA] §6.3.2, Appendix A (10) & (11)
			2.18	**Copied Containers**		
Security	Required	86	2.18.1	The system recognizes when the FASC-N in the CHUID does not equal the FASC-N in the PKI-CAK Cert	Card 16: (FASC-N in CHUID !=) fails to register successfully	PIA-3.2; [SP800-73], Part 1, §3.1.2
Security	Required	87	2.18.2	The system recognizes when the UUID in the CHUID does not equal the UUID in the PIV-I Auth Cert	Card 20: (UUID in CHUID !=) fails to register successfully	PIA-3.2; [SP800-73], Part 1, §3.1.2
			2.19	**Signature Verification (Contactless chip on a 2 chip card)**	**These tests are run using a contactless reader. PKI-CAK mode is used for all tests.**	
Security	Required	88	2.19.1	Verify products ability to validate signatures in the certificates found in the certification path for a PIV credential	Card 1: PIV Golden Registers successfully as second valid certificate for PKI-CAK.	PIA-2 thru PIA-7
Security	Required	89	2.19.2	Verify products ability to validate signatures in the certificates found in the certification path for a PIV-I credential	Card 2: PIV-I Golden Registers successfully as second valid certificate for PKI-CAK.	PIA-2 thru PIA-7
Security	Required	90	2.19.3	Verify products ability to recognize invalid signature on an intermediate CA in the	Card 1: (Golden PIV Card) w/ PKI Fault Bridge 2.1.2 fails to register successfully.	PAI-3.2, PIA-3.4, PIA-4,

				certification path		PIA-5
Security	Required	91	2.19.4	Verify products ability to recognize invalid signature on the End Entity certificate	Card 5: invalid Card Auth Signer fails to register successfully.	PAI-3.2, PIA-3.4, PIA-4
Security	Required	92	2.19.5	Verify products ability to recognize certificate/private key mismatch	Card 23: Certificate Private Key mismatch fails to register successfully.	PAI-3.2, PIA-3.4, PIA-4
				NFC Devices	**All new requirements/tests**	
				Not tested unless and until FIPS 201-2 defines requirements for derived credentials that can be enabled on NFC devices.		
			3	**Requirements for Automated Provisioning In Accordance With [E-PACS] PIA-8**	NEW Section: Certainly need to consider what a Spec btw E-IdM and PACS would look like to provide testable requirements.	Moved from PACS Design section here. Clarifies recognition of both registration models (in person, E-IdM sourced).
			3.1	**Dual Interface Chip Card**		

Security	Optional	*93*	3.1.1	The E-PACS shall accept automated provisioning from a source it trusts and that complies with the security requirements described in the detailed guidance of PIA-8.	Perform design analysis of automated provisioning functionality of the solution.	PIA-8; [Roadmap], §9.2.3.1 including Figure 94
Security	Optional	*94*	3.1.2	The E-PACS shall accept automated deprovisioning from a source it trusts and that complies with the security requirements described in PIA-3.5 and PIA-3.6.	Perform design analysis of automated deprovisioning functionality of the solution.	PIA-8, PIA-3.5, PIA-3.6; [Roadmap], §9.2.3.1 including Figure 94
			3.2	**Dual Chip Card**	All new requirements/tests	[FIPS 201] allows dual chip cards.
Security	Optional	*95*	3.2.1	The E-PACS shall accept automated provisioning of the contactless CAK from a source it trusts and that complies with the security requirements described in the detailed guidance of PIA-8.	Perform design analysis of automated provisioning functionality of the solution.	PIA-8; [Roadmap], §9.2.3.1 including Figure 94
Security	Optional	*96*	3.2.2	The E-PACS shall accept automated deprovisioning of the contactless CAK from a source it trusts and that complies with the security requirements described in PIA-3.5 and PIA-3.6.	Perform design analysis of automated deprovisioning functionality of the solution.	PIA-8, PIA-3.5, PIA-3.6; [Roadmap], §9.2.3.1 including Figure 94
			4	**Authentication at Time of Access Test Cases**	All tests use PKI-AUTH unless specifically noted.	Need to add caching/temporal aspect to these PKI tests at time of access.

			4.1	**Signature Verification**		
Security	Required	97	4.1.1	Verify products ability to validate signatures in the certificates found in the certification path for a PIV credential	Card 1: PIV Golden Receives an access grant Successfully	PIA-2 thru PIA-7
Security	Optional	98	4.1.2	Verify products ability to validate signatures in the certificates found in the certification path for a PIV-I credential	Card 2: PIV-I Golden Receives an access grant Successfully	PIA-2 thru PIA-7
Security	Required	99	4.1.3	Verify products ability to recognize invalid signature on an intermediate CA in the certification path	Card 1: (Golden PIV Card) w/ PKI Fault Bridge 2.1.2 fails to receive an access grant	PAI-3.2, PIA-3.4, PIA-4, PIA-5
Security	Required	100	4.1.4	Verify products ability to recognize invalid signature on the End Entity certificate	Card 5: invalid PIV/Card Auth Signer fails to receive an access grant	PAI-3.2, PIA-3.4, PIA-4
			4.2	**Certificate Validity Periods**		
Security	Required	101	4.2.1	Verify products ability to reject a credential when notBefore date of the intermediate CA certificate is sometime in the future	Card 1: (Golden PIV Card) fails access grant w/ PKI Fault Bridge 2.2.1	PIA-3.5, PIA-5
Security	Required	102	4.2.2	Verify products ability to reject a credential when notBefore date of the End Entity certificate is sometime in the future	Card 12: (Certs not yet valid) access grant fails	PIA-3.5
Security	Required	103	4.2.3	Verify products ability to reject a credential when notAfter date of the intermediate certificate is sometime in the past	Card 1: (Golden PIV Card) fails access grant w/ PKI Fault Bridge 2.2.3	PIA-3.5, PIA-5
Security	Required	104	4.2.4	Verify products ability to reject a credential when notAfter date of the End Entity certificate is sometime in the past	Card 13: (Certs Expired) access grant fails	PIA-3.5
			4.3	**Name Chaining**		

Security	Required	105	4.4.1	Verify products' ability to reject a credential when common name portion of the of the issuer's name in the End Entity certificate does not match common name portion of subject's name in the previous intermediate certificate	Card 1: (Golden PIV Card) fails access grant w/ PKI Fault Bridge 2.3.1	PIA-3.2, PIA-5
			4.4	**Basic Constraints Verification**		
Security	Required	106	4.4.1	Verify product's ability to recognize when the intermediate CA certificate is missing basicConstraints extension.	Card 1: (Golden PIV Card) fails access grant w/ PKI Fault Bridge 2.4.1	PIA-3.2, PIA-5
Security	Required	107	4.4.2	Verify product's ability to recognize when the basicConstraints extension is present and critical in the intermediate CA certificate but the CA component is false	Card 1: (Golden PIV Card) fails access grant w/ PKI Fault Bridge 2.4.2	PIA-3.2, PIA-5
Security	Required	108	4.4.3	Verify product's ability to recognize when the basicConstraints extension is present and not critical in the intermediate CA certificate but the CA component is false	Card 1: (Golden PIV Card) fails access grant w/ PKI Fault Bridge 2.4.3	PIA-3.2, PIA-5
Security	Required	109	4.4.4	Verify product's ability to recognize when the first certificate in the path includes basicConstraints extension with a pathLenConstraint of 0 (this prevents additional intermediate certificates from appearing in the path). The first certificate is followed by the second intermediate CA certificate and an End Entity certificate.	Card 1: (Golden PIV Card) fails access grant w/ PKI Fault Bridge 2.4.4	PIA-3.2, PIA-5
			4.5	**Key Usage Verification**		

Security	Required	110	4.5.1	Verify products ability to recognize when the intermediate certificate includes a critical keyUsage extension in which keyCertSign is false	Card 1: (Golden PIV Card) fails access grant w/ PKI Fault Bridge 2.5.1	PIA-3.2, PIA-5
Security	Required	111	4.5.2	Verify products ability to recognize when the intermediate certificate includes a non-critical keyUsage extension	Card 1: (Golden PIV Card) fails access grant w/ PKI Fault Bridge 2.5.2	PIA-3.2, PIA-5
Security	Required	112	4.5.3	Verify products ability to recognize when the intermediate certificate includes a critical keyUsage extension in which cRLSign is false	Card 1: (Golden PIV Card) fails access grant w/ PKI Fault Bridge 2.5.3	PIA-3.2, PIA-5
			4.6	**Certificate Policies**		
Security	Required	113	4.6.1	With the trust anchor set to Common Policy check to see if the validation software is able to recognize when an explicit certificate policy is required and present in the certificate path. The explicit policy will be set to PIV Hardware.	Production PIV receives access grant	PIA-3.2, PIA-5
Security	Required	114	4.6.2	With the trust anchor set to Common Policy check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the certificate path. The explicit policy will be set to an arbitrary value that is not present in the certificate path (ex., OID value 1.2.3.4).	Production PIV receives access denied	PIA-3.2, PIA-5

Security	Required	115	4.6.3	With the trust anchor set so the certificate path requires trust across the Federal Bridge to the CertiPath Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and present in the certificate in a bridged trust environment. The explicit policy will be set to Medium Hardware. Test Condition: production PIV passes	Production PIV receives access grant	PIA-3.2, PIA-5
Security	Required	116	4.6.4	With the trust anchor set so the certificate path requires trust across the Federal Bridge to the CertiPath Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the certificate in a bridged trust environment. The explicit policy will be set to an arbitrary value that is not present in the certificate chain (ex., OID value 1.2.3.4).	Production PIV receives access denied	PIA-3.2, PIA-5
Security	Required	117	4.6.5	With Common Policy anchor, check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the certificate - however, is present somewhere in the certificate path. The explicit policy will be set to a value that is present in the certificate path, but does not map to the end entity certificate (ex, High Hardware).	Production PIV receives access denied	PIA-3.2, PIA-5
			4.7	**Inhibit Policy Mappings**		

Security	Required	118	4.7.1	The first intermediate certificate asserts NIST-test-policy-1 and includes a policyConstraints extension with inhibitPolicyMapping set to 0. The second intermediate certificate asserts Policy A and maps Policy A to Policy B. The end entity certificate asserts Policy A and Policy B	Card 1: (Golden PIV Card) fails access grant w/ PKI Fault Bridge 2.5.3	PIA-3.2, PIA-5
			4.8	**Name Constraints**		
Security	Required	119	4.8.1	The system recognizes when the intermediate certificate includes a nameConstraints extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls within that subtree.	Card 1: (PIV Golden) access grant succeeds	PIA-3.2, PIA-5
Security	Required	120	4.8.2	The system recognizes when the intermediate certificate includes a nameConstraints extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls outside that subtree.	Card 1: (Golden PIV Card) fails access grant w/ PKI Fault Bridge 2.10.2	PIA-3.2, PIA-5
Security	Required	121	4.8.3	The system recognizes when the intermediate certificate includes a nameConstraints extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls within that subtree and subjectAltName with a DN that falls outside that subtree.	Card 1: (Golden PIV Card) fails access grant w/ PKI Fault Bridge 2.10.1	PIA-3.2, PIA-5
			4.9	**Certificate Revocation Tests (CRL)**		
Security	Required	122	4.9.1	The system recognizes when no revocation information is available for the End Entity certificate	Card 1: (Golden PIV Card) fails access grant w/ PKI Fault Bridge 2.11.1	PIA-3.5, PIA-5, PIA-7

Security	Required	123	4.9.2	The system recognizes when a second intermediate CA certificate is revoked	Card 1: (Golden PIV Card) fails access grant w/ PKI Fault Bridge 2.11.2	PIA-3.5, PIA-5, PIA-7
Security	Required	124	4.9.3	The system recognizes when the End Entity certificate is revoked	Card 24: Revoked status	PIA-3.5, PIA-5, PIA-7
Security	Required	125	4.9.4	The system recognizes when the CRL has an invalid signature	Card 1: (Golden PIV Card) fails access grant with Path 17	PIA-3.5, PIA-5, PIA-7
Security	Required	126	4.9.5	The system recognizes when a certificate in the path links to a CRL issued by a CA other than that which issued the cert	Card 1: (Golden PIV Card) fails access grant w/ PKI Fault Bridge 2.11.5	PIA-3.5, PIA-5, PIA-7
Security	Required	127	4.9.6	The system recognizes when a certificate in the path has an expired nextUpdate value	Card 1: (Golden PIV Card) fails access grant w/ PKI Fault Bridge 2.11.6	PIA-3.5, PIA-5, PIA-7
Security	Required	128	4.9.7	The system recognizes when a certificate in the path points to a CRL with a notBefore Date in the future.	Card 1: (Golden PIV Card) fails access grant w/ PKI Fault Bridge 2.11.7	PIA-3.5, PIA-5, PIA-7
Security	Required	129	4.9.8	The system recognizes when a certificate in the path has an incorrect distribution point	Card 1: (Golden PIV Card) fails access grant w/ PKI Fault Bridge 2.11.8	PIA-3.5, PIA-5, PIA-7
			4.10	**CHUID Verification**	See 4.3.1: If CHUID Auth Meth is Supported, tests in this section are Required.	
Security	Required	130	4.10.1	The system recognizes when the CHUID signature is invalid and does not verify	Card 4: (Invalid CHUID Signature) fails access grant	PIA-3.2, PIA-4
Security	Required	131	4.10.2	The system recognizes when the CHUID signer certificate is expired	Card 9: (Expired CHUID signer) fails access grant	PIA-3.6, PIA-5
Security	Required	132	4.10.3	The system recognizes when the CHUID is expired	Card 14: (Card Expired) fails access grant	PIA-3.6

			4.11	**Facial Image Verification**	If showing facial image as part of an access transaction is Supported, tests in this section are Required.	Need CHUID content signer? Or SecObj? Or in facial buffer?
Security	Required	133	4.11.1	The system recognizes when the Facial Image signature is invalid and does not verify.	Card 6: (bad photo signature) fails access grant	PIA-3, PIA-3.2, PIA-3.3, PIA-4
			4.12	**FINGERPRINT Verification**	See 4.3.4: If BIO Auth Meth is Supported, tests in this section are Required. If content signer certificate is from CHUID, Section 3.10 is Required.	
Security	Required	134	4.12.1	The system recognizes when the Fingerprint signature is invalid and does not verify (using CHUID content signer certificate).	Card 7: (bad fingerprint signature) access grant fails	PIA-3, PIA-3.2, PIA-3.3, PIA-4
Security	Required	135	4.12.1	The system recognizes when the Fingerprint signature is invalid and does not verify (using biometric object signer certificate).	Card xx: (bad fingerprint signature) fails to register successfully	PIA-3.2, PIA-3.4, PIA-3.5, PIA-3.6, PIA-4, PIA-5
Security	Required	136	4.12.2	Verify Product's ability to accept a valid credential with a matching fingerprint.	A good credential is presented to the system with a valid fingerprint object on card. System is presented correct bearer's fingerprint. Access is granted.	PIA-3 thru PIA-7
Security	Required	137	4.12.3	Verify Product's ability to reject a valid credential with a non-matching fingerprint.	A good credential is presented to the system with a valid fingerprint object on card. System is presented incorrect bearer's fingerprint. Access grant fails.	PIA-3.3
			4.13	**Security Object Verification**	If Security Object is Supported, tests in this section are Required.	

Security	Required	138	4.14.1	The system recognizes when the Security Object signature is invalid and does not verify.	Card 8: (bad security object signature) access grant fails	PIA-3.4, PIA-4, PIA-5
			4.14	**OCSP Response Checking**		
Security	Required	139	4.14.1	The system successfully validates a good credential using an OCSP response with a good signature	Card 1: Golden PIV is granted access	PIA-3.2, PIA-3.5
Security	Required	140	4.14.2	Validation fails using an OCSP responder with an expired signature certificate for a good card.	Card 1: Golden PIV access is denied	PIA-3.2 PIA-3.5, PIA-3.6
Security	Required	141	4.14.3	Validation succeeds using an OCSP responder with a revoked signature certificate for a good card with PKIX_OCSP_NOCHECK present.	Card 1: Golden PIV is granted access	PIA-3.2, PIA-3.5
Security	Required	142	4.14.4	Validation fails using an OCSP responder with a revoked signature certificate for a good card without PKIX_OCSP_NOCHECK present.	Card 1: Golden PIV access is denied	PIA-3.2, PIA-3.5, PIA-3.6
Security	Required	143	4.14.5	Validation fails using an OCSP responder with a signature certificate containing an invalid signature for a good card.	Card 1: Golden PIV access is denied	PIA-3.2, PIA-4
			4.15	**Interoperability Testing**	Tests in this section attempt to use a variety of dual interface production PIV and PIV-I cards in the system.	
Usability	Required	144	4.15	Various valid PIV (including CAC) and PIV-I cards are granted access using PKI-AUTH method.	PIV (including CAC) and PIV-I cards are granted access	PIA-6
			4.16	**Cryptography testing**	As stated, there is no context for challenge/response vs. use of crypto w/in certs and path for sigval. The FICAM Testing Program will isolate these two	

					variables in new test cases.	
Security	Required	145	4.16.1	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (1024).	NIST card#7 is granted access.	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5
Security	Required	146	4.16.2	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (2048).	NIST card#1 is granted access.	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5
Security	Required	147	4.16.3	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (3072).	TBD	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5
Security	Optional	148	4.16.4	Verify Product's ability to validate signatures using RSASSA-PSS (1024).	TBD (valid through 1/1/2014)	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5

Security	Optional	149	4.16.5	Verify Product's ability to validate signatures using RSASSA-PSS (2048).	NIST card#2 is granted access.	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5
Security	Optional	150	4.16.6	Verify Product's ability to validate signatures using RSASSA-PSS (3072).	TBD	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5
Security	Optional	151	4.16.7	RSA Key Transport (1024)	TBD (valid through 1/1/2014)	[SP800-78] Table 3-1
Security	Optional	152	4.16.8	RSA Key Transport (2048)	TBD	Derived from [SP800-78] Table 3-1 and [Common] §6.1.5
Security	Optional	153	4.16.9	RSA Key Transport (3072)	TBD	Derived from [SP800-78] Table 3-1 and [Common] §6.1.5
Security	Required	154	4.16.10	Verify Product’s ability to validate signatures using ECDSA (P-256)	NIST card#4 is granted access.	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5

Security	Optional	155	4.16.11	Verify Product's ability to validate signatures using ECDSA (P-384)	NIST card#5 is granted access.	[SP800-78] Table 3-1; [SP800-78] Table 3-3; [Common] §6.1.5
Security	Optional	156	4.16.12	ECDH (P-256)	TBD	[SP800-78] Table 3-1; [Common] §6.1.5
Security	Optional	157	4.16.13	ECDH (P-384)	TBD	[SP800-78] Table 3-1; [Common] §6.1.5
Security	Optional	158	4.16.14	Verify Product's ability to validate signatures using SHA-1	NIST card#7 is granted access.	[SP800-78] Table 3-7; [Common] §6.1.5
Security	Required	159	4.16.15	Verify Product's ability to validate signatures using SHA-256	NIST card#1 is granted access.	[SP800-78] Table 3-7; [Common] §6.1.5
Security	Optional	160	4.16.16	Verify Product's ability to validate signatures using SHA-384	NIST card#5 is granted access.	[SP800-78] Table 3-7; [Common] §6.1.5
Security	Optional	161	4.16.17	Verify Product's ability for SYM-CAK using AES-128	TBD	[SP800-73] table 3-1; [Common] §6.1.5

Security	Optional	162	4.16.18	Verify Product's ability for SYM-CAK using AES-192	TBD	[SP800-73] table 3-1; [Common] §6.1.5
Security	Optional	163	4.16.19	Verify Product's ability for SYM-CAK using AES-256	TBD	[SP800-73] table 3-1; [Common] §6.1.5
Security	Optional	164	4.16.20	Verify Product's ability for SYM-CAK using 2TDEA	TBD	[SP800-73] table 3-1; [Common] §6.1.5
Security	Optional	165	4.16.21	Verify Product's ability for SYM-CAK using 3TDEA	TBD	[SP800-73] table 3-1; [Common] §6.1.5
Security	Required	166	4.16.22	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (2048) w/exponent of 65,537.	NIST card#1 is granted access.	[SP800-78] Table 3-2
Security	Optional	167	4.16.23	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (2048) w/exponent of 2^256-1.	TBD	[SP800-78] Table 3-2
			4.17	**Continuity of Operations Testing**		
Usability	Optional	168	4.17.1	The network connection is dropped to individual components within the solution individually, in sequence. Degraded mode shall honor requirements for authentication factors and authorizations for a valid credential.	For each component within a solution, disconnect the network to the component. Using Test Card 1: Golden, document success/failure.	PCP-1

Usability	Optional	169	4.17.2	Individual component services within the solution are stopped individually, in sequence. Degraded mode shall honor requirements for authentication factors and authorizations for a valid credential.	For each service within a solution, manually stop the service on the server(s). Test Card 1: PIV Golden, document success/failure.	PCP-1
Usability	Optional	170	4.17.3	Power is removed and immediately restored to individual components within the solution, in sequence. Solution shall recover and honor requirements for authentication factors and authorizations for a valid credential.	For each component within the solution, abruptly remove all power sources from the power supply. Restore power. Attempt access with Test Card 1: PIV Golden, document success/failure.	PCP-1
Usability	Optional	171	4.17.4	The network connection is dropped to individual components within the solution individually, in sequence. Degraded mode shall honor requirements for authentication factors and authorizations for an invalid credential.	For each component within a solution, disconnect the network to the component. Using Test Card 13: Expired PIV Auth, document success/failure.	PCP-1
Usability	Optional	172	4.17.5	Individual component services within the solution are stopped individually, in sequence. Degraded mode shall honor requirements for authentication factors and authorizations for an invalid credential.	For each service within a solution, manually stop the service on the server(s). Test Card 13: Expired PIV Auth, document success/failure.	PCP-1
Usability	Optional	173	4.17.6	Power is removed and immediately restored to individual components within the solution, in sequence. Solution shall recover and honor requirements for authentication factors and authorizations for an invalid credential.	For each component within the solution, abruptly remove all power sources from the power supply. Restore power. Attempt access with Test Card 13: Expired PIV Auth, document success/failure.	PCP-1
			5	**PACS Design Use Cases**		

			5.1	**Security Boundaries**		
Security	Required	174	5.1.1	...all security relevant processing shall be performed inside the secure perimeter. No security relevant decisions shall be made by system components that do not belong to the cardholder's credential when they are on the attack side of the door.	Confirm all PACS components (except for the reader and the bearer's credential) are capable of being located on the secure side of perimeter. Confirm with protocol sniffing between secure/attack side	PPE-1
Security	Optional	175	5.1.2	...compensating controls applied such as tamper switches and FIPS 140-2 certified cryptographic processing within the reader itself.	Specific waivers to 4.1.1 shall be granted on a per implementation basis of compensating controls. Document all supplemental security devices and check against APLs, FIPS 140-2. Confirm controls are operational through physical inspection, design documentation. Confirm with protocol sniffing between secure/attack side.	PPE-1
			5.2	**Registering Physical Access Privileges**		
Usability	Optional	176	5.2.1	Shall be able to define populations (validities) such as "guest, visitor, regular access".	Confirm physical inspection and design documentation.	PPL-4
Usability	Optional	177	5.2.2	shall be able to define: Access points for each population	Verify by system design review	PPL-5, PAC-1
Usability	Optional	178	5.2.3	shall be able to define: Temporal access rules for each population	Verify by system design review	PPL-5, PAC-1
Usability	Optional	179	5.2.4	shall be able to define: Authentication mode required to support 4.2.2 and 4.2.3	Verify by system design review	PPL-5, PAC-1
Security	Required	180	5.2.5	No credential shall be individually registered for which there is no valid trust path per the relying party PKI policy.	Derive from the overall results of testing in Section 2.	PIA-9

Security	Required	181	5.2.5	No credential shall be individually registered where the binding of the credential to the bearer does not meet relying party security policy.	Derive from the overall results of testing in Section 2.	PIA-9
Security	Required	182	5.2.5	No credential shall be individually authorized for access that does not meet relying party security policy.	Derive from the overall results of testing in Section 2.	PIA-9
			5.3	**PKI Configuration**		
Security	Optional	183	5.3.1	The solution shall provide the means to select which X.509 constraints are evaluated such as policy constraints, name constraints and key usage. This configuration will reflect the customer's PKI relying party policy.	Verify configurability of X.509 constraints and policies.	PIA-5
Security	Required	184	5.3.2	The solution shall provide the means to select and manage Trust Anchors. This configuration will reflect the customer's PKI relying party policy.	Verify configurability of trust anchors.	PSC-2
			5.4	**Credential number specifications**		
Usability	Required	185	5.4.1	Credential number specifications are being developed by the FICAM Testing Program for use in Spiral 1.		PAU-2, PAU-3; Table 6-1 row 3
			5.5	**Validation at Time of Access**		
Usability	Optional	186	5.5.1	Shall support Signed CHUID	Use Authentication Test logs to verify that all good cards were allowed access at the door reader.	PIA-2, PIA-3.x, PIA-4, PIA-5, PIA-6, PIA-7
Usability	Optional	187	5.5.2	Shall support contactless Card Authentication Key (PKI-CAK) for Dual Interface Chip card	Use Authentication Test logs to verify that all good cards were allowed access at the door reader.	PIA-2, PIA-3.x, PIA-4, PIA-5, PIA-6, PIA-7

Usability	Optional	188	5.5.3	Shall support BIO	Use Authentication Test logs to verify that all good cards with valid BIO available were allowed access at the door reader.	PIA-2, PIA-3.x, PIA-4, PIA-5, PIA-6, PIA-7
Usability	Optional	189	5.5.4	Shall support PIV Authentication Key + PIN (PKI-AUTH)	Use Authentication Test logs to verify that all good cards were allowed access at the door reader.	PIA-2, PIA-3.x, PIA-4, PIA-5, PIA-6, PIA-7
Usability	Optional	190	5.5.5	Shall support PIV Authentication Key + PIN + BIO (PKI-AUTH+BIO)	Use Authentication Test logs to verify that all good cards with valid PKI-AUTH and BIO available were allowed access at the door reader.	PIA-2, PIA-3.x, PIA-4, PIA-5, PIA-6, PIA-7
Usability	Optional	191	5.5.6	Shall support Card Authentication Key + PIN + BIO (PKI-CAK+BIO)	Use Authentication Test logs to verify that all good cards with valid PKI-CAK and BIO available were allowed access at the door reader.	PIA-2, PIA-3.x, PIA-4, PIA-5, PIA-6, PIA-7
Usability	Optional	192	5.5.7	Shall support PKI-CAK + BIO to PACS	Use Authentication Test logs to verify that all good cards with valid BIO were allowed access at the door reader. Confirm protection of authenticator in the PACS.	PIA-2, PIA-3.x, PIA-6, PIA-3.4 Detailed Guidance Case 3
Usability	Optional	193	5.5.8	Shall support PKI-AUTH + BIO to PACS	Use Authentication Test logs to verify that all good cards with valid BIO were allowed access at the door reader. Confirm protection of authenticator in the PACS.	PIA-2, PIA-3.x, PIA-6, PIA-3.4 Detailed Guidance Case 3
Usability	Optional	194	5.5.9	Shall support contact Card Authentication Key (PKI-CAK) for Dual Interface Chip card	Use Authentication Test logs to verify that all good cards were allowed access at the door reader.	PIA-2, PIA-3.x, PIA-4, PIA-5, PIA-6, PIA-7
Usability	Optional	195	5.5.10	Shall support contactless Card Authentication Key (PKI-CAK) for Dual Chip card	Use Authentication Test logs to verify that all good cards were allowed access at the door reader.	PIA-2, PIA-3.x, PIA-4, PIA-5, PIA-6, PIA-7

			5.6	**Portal Hardware**		
Security	Required	196	5.6.1	Product shall support Reader to PACS communications using bi-directional technology. This includes a minimum of one of RS-485, Ethernet, secure wireless.	Verify by system design review. Confirmed using protocol sniffing, review of logs produced during authentication testing.	PCM-2, PCM-3
Usability	Optional	197	5.6.2	For multi-factor readers, applicant's system must allow an administrator to modify an individual reader's authentication mode (authentication factors) from the server or a client/workstation to the server.	Verify by system design review. Confirm by setting multi-factor reader authentication modes and using Test card 1: PIV Golden for access according to mode.	PCM-3
Usability	Optional	198	5.6.2	For multi-factor readers, applicant's system must allow an administrator to modify a group of readers' authentication mode (authentication factors) from the server or a client/workstation to the server.	Verify by system design review. Confirm by setting multi-factor reader authentication modes and using Test card 1: PIV Golden for access according to mode.	PCM-3
Usability	Optional	199	5.6.3	For multi-factor readers, the site administrator shall not be required to approach and touch each reader to change its authentication mode (authentication factors).	Verify by system design review. Confirm by setting multi-factor reader authentication modes and using Test card 1: PIV Golden for access according to mode.	PCM-3
Usability	Optional	200	5.6.4	For multi-factor readers, the system shall support dynamic assignment an individual reader's authentication mode (authentication factors) on a time based schedule.	Verify by system design review. Confirm by setting schedule for multi-factor reader authentication modes and using Test card 1: PIV Golden for access according to mode.	PCM-3
Usability	Optional	201	5.6.5	For multi-factor readers, the system shall support dynamic assignment a group of readers' authentication mode (authentication factors) on a time based schedule.	Verify by system design review. Confirm by setting schedule for multi-factor reader authentication modes and using Test card 1: PIV Golden for access according to mode.	PCM-3

Usability	Optional	202	5.6.6	For multi-factor readers, the system shall support dynamic assignment of an individual reader's authentication mode (authentication factors) based on Threat Condition, Force Protection Condition, Maritime Security Level, or other similar structured emergency response protocol.	Verify by system design review. Confirm by setting emergency response protocol level for multi-factor reader authentication modes and using Test card 1: PIV Golden for access according to mode.	PCM-3
Usability	Optional	203	5.6.7	For multi-factor readers, the system shall support dynamic assignment of a group of readers' authentication mode (authentication factors) based on Threat Condition, Force Protection Condition, Maritime Security Level, or other similar structured emergency response protocol.	Verify by system design review. Confirm by setting emergency response protocol level for multi-factor reader authentication modes and using Test card 1: PIV Golden for access according to mode.	PCM-3
Usability	Optional	204	5.6.8	Contact readers shall support ISO/IEC 7816.	The contact interface of the reader shall be tested for ISO/IEC 7816 conformance. It is recommended the vendor test in accordance with ISO/IEC 10373-3:2010 Sections 4, 7, and 8. Vendor shall provide a test data report documenting conformance for review and approval.	[FIPS 201]
Usability	Optional	205	5.6.9	Contactless readers shall support ISO/IEC 14443 Type A.	The contactless interface of the reader shall be tested for ISO/IEC 14443 Type A conformance. It is recommended the vendor test in accordance with ISO/IEC 10373-6:2011 Sections 4, 5, 6.1, 7.1 and 8.1, and ISO/IEC 10373-6:2011/Amd.4:2012. Vendor shall provide a test data report documenting conformance for review and approval.	[FIPS 201]

Usability	Optional	206	5.6.10	ISO/IEC 14443 Type B protocols are deprecated. When a Type B card is presented, the reader shall reject the card.	NIST card 3 is presented to the reader. The reader shall reject the card.	FICAM Testing Program; Updated [SP800-96] to be published by NIST after FIPS 201-2.
Security	Required	207	5.6.11	ISO/IEC 14443 Type A contactless readers shall not activate and operate with a PIV card beyond 10cm.	Card 1 is presented at 11cm to the reader. All contactless PIV authentication modes shall fail.	[FIPS 201]
Usability	Required	208	5.6.12	ISO/IEC 14443 Type A contactless readers shall provide sufficient field strength to activate and operate with a PIV card at or below 7cm.	Card 1 is presented at 7cm to the reader. All contactless PIV authentication modes shall succeed.	[FIPS 201]
Security	Optional	209	5.6.13	The System shall protect the communications between readers and the PACS using a cryptographically secure protocol.	FICAM profile for OSDP to be developed in next spiral of FICAM Testing Program.	PSC-1
Usability	Optional	210	5.6.14	For multi-factor readers, if a time delay of longer than 120 seconds is required for a reader to change modes, this too shall be considered non-compliant.	Verify by system design review	PCM-3
			5.7	**Auditing and Logging**		
Security	Required	211	5.7.1	Granularity of auditing records shall be to the card and individual transaction. These shall be easily verifiable through a reporting tool or any other log and audit viewing capability	Verify by review of logs and reports	PAU-1, PAU-2, PAU-7

Security	Required	212	5.7.2	The product shall provide auditing/logging of all PKI processing to include - Pass/fail from a Challenge/Response - PDVAL - Disabling credential based on PDVAL, expiration or revocation status	Verify by review of logs and reports; confirmed by protocol sniffing	PAU-3, PAU-4, PAU-7
Security	Required	213	5.7.3	The product shall provide auditing/logging of credential number processing and transmission	Verify by review of logs and reports	PAU-4, PAU-5, PAU-7
Security	Required	214	5.7.4	The product shall provide auditing/logging of all software driven configuration changes	Verify by review of logs and reports	PAU-6, PAU-7
Security	Required	215	5.7.5	The product shall provide auditing/logging of periodic certificate PDVAL and status checking	Verify by review of logs and reports	PAU-4, PAU-5, PAU-7
Security	Required	216	5.7.6	The product shall provide auditing/logging of Card activity (e.g., 3 days of card activity)	Verify by review of logs and reports	PAU-3, PAU-7
Security	Required	217	5.7.7	The product shall provide auditing/logging of last known location of a card in system	Verify by review of logs and reports	PAU-3, PAU-7
Security	Required	218	5.7.8	The product shall provide auditing/logging of PKI policies for name constraints, path constraints, validity checks	Verify by review of logs and reports	PAU-4, PAU-5, PAU-7
Security	Required	219	5.7.9	The product shall provide auditing/logging of individual and group reporting of alarms (e.g., door force, door prop)	Verify by review of logs and reports	PAU-3, PAU-7
Security	Required	220	5.7.10	The product shall provide auditing/logging of what date individuals were provisioned or de-provisioned and by whom	Verify by review of logs and reports	PAU-4, PAU-7
Security	Required	221	5.7.11	The product shall provide auditing/logging of all readers and their modes	Verify by review of logs and reports	PAU-5, PAU-6, PAU-7

Security	Required	222	5.7.12	The product shall provide auditing/logging of configuration download status to system components	Verify by review of logs and reports	PAU-5, PAU-6, PAU-7
			5.8	**Security Certification and Accreditation**		
Usability	Required	223	5.8.1	As required by UL 294, relevant components within the solution shall have a UL 294 listing	Verify UL listing. Must be listed before final testing and certification by GSA FIPS 201 APL program.	PCA-2
Usability	Required	224	5.8.2	When adding a component to an existing system under a given topology, each existing component in the existing system under that topology shall have GSA FIPS-201-1 APL status.	Verify APL listing. Must be listed before final testing and certification by GSA FIPS 201 APL program.	PCA-3
Security	Required	225	5.8.3	Each component leveraging cryptography in the system shall have FIPS 140-2 certification.	Verify NIST CMVP listing. Must be applied for and in process for certification before any testing can be done. Must be listed before final testing and certification by GSA FIPS 201 APL program.	PCA-4
			5.9	**Biometric in PACS**		
Security	Optional	226	5.9.1	Shall follow PIA-3.4 Detailed Guidance Case 3 for biometric identifiers leveraged in BIO to PACS.	Verify by system design and inspection of database	PIA-3.4
			5.1	**Operational Controls**		
Security	Required	227	5.10.1	The system shall have the ability to enforce administrative privilege for configuration management operations.	Verify by use of the system.	PCM-1

Security	Required	228	5.10.2	Shall authenticate administrators using a process of equivalent or greater assurance than the authentication modes supported by the system. This may be done using E-Auth LOA-4 credentials.	Verify by use of the system.	PCM-1
Usability	Optional	229	5.10.3	The system shall have the ability to manage the system through software controlled configuration management methods. Initial configuration of hardware settings (e.g., DIP switches) is allowed at installation only and not for management of the hardware tree	Verify by use of the system.	PCM-2
Usability	Optional	230	5.10.4	Each physical component shall be separately defined and addressable within the server user interface	Verify by setting up of system.	PCM-2
Usability	Optional	231	5.10.5	The system shall support configuration downloads to relevant components	Verify by setting up of system.	PCM-2
			6	**Optional TRANSITIONAL Technologies for Addition to the FICAM Reader**		
Usability	Optional	232	6.1.1	The system shall support 125KHz credentials		
Usability	Optional	233	6.1.2	The system shall support iClass credentials		
Usability	Optional	234	6.1.3	Transparent FASC-N (PIV)		
Usability	Optional	235	6.1.4	Transparent UUID (PIV-I)		

Security	Optional	236	6.1.5	Legacy technology credential number specifications are being developed by the FICAM Testing Program for use in Spiral 1.		PAU-2, PAU-3
Usability	Optional	237	6.1.6	Product shall support Reader to Panel communications using uni-directional Wiegand	Confirm availability of Weigand wiring/connector from reader. Hook up reader to panel and confirm protocol operations.	
Usability	Optional	238	6.1.7	Product shall support Reader to Panel communications using bi-directional RS-485	Confirm availability of RS-485 wiring/connector from reader. Hook up reader to panel and confirm protocol operations.	PCM-3
Usability	Optional	239	6.1.8	Product may support secure wireless communications in lieu of or in addition to both R-FTR-6 and R-FTR-7	Confirm availability of secure wireless from reader. Establish connection from reader to wireless hub and confirm protocol operations.	PCM-3
Usability	Optional	240	6.1.9	Shall support BIO	Use Authentication Test logs to verify that all good cards with valid BIO available were allowed access at the door reader.	PIA-2, PIA-3.x, PIA-4, PIA-5, PIA-6
Security	Optional	241	6.1.10	The System shall protect the communications between readers and the PACS using a cryptographically secure protocol.	FICAM profile for OSDP to be developed in next spiral of FICAM Testing Program.	PSC-1
Usability	Optional	242	6.1.11	The system shall support Mifare credentials		
Usability	Optional	243	6.1.12	The system shall support DESFire V6 (D40 chip) credentials		